EXHIBIT A

USPTO Patent 7003500

"3500 patent"

US007003500B1

(12) **United States Patent**
Driessen

(10) **Patent No.: US 7,003,500 B1**
(45) **Date of Patent: Feb. 21, 2006**

(54) **RETAIL POINT OF SALE (RPOS) APPARATUS FOR INTERNET MERCHANDISING**

(76) Inventor: **James Leonard Driessen**, 305 N 1130 E, Lindon, UT (US) 84042

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1068 days.

(21) Appl. No.: **09/630,272**

(22) Filed: **Aug. 1, 2000**

(51) **Int. Cl.**
G06F 17/60 (2006.01)
H04K 1/00 (2006.01)
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **705/74**; 705/64

(58) **Field of Classification Search** 705/26, 705/51, 58, 64, 70, 74; 380/201, 202
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,033,184	A	7/1991	Tandai et al.	29/603.06
5,339,239	A	8/1994	Manabe et al.	705/1
5,530,751	A *	6/1996	Morris	380/202
5,568,550	A	10/1996	Ur	382/306
5,629,770	A *	5/1997	Brassil et al.	358/426.12
5,699,427	A	12/1997	Chow et al.	705/58
5,745,569	A	4/1998	Moskowitz et al.	705/98
5,777,305	A	7/1998	Smith et al.	235/380
5,899,700	A *	5/1999	Williams et al.	434/308
5,905,248	A	5/1999	Russell et al.	235/462.15
5,920,878	A	7/1999	DeMont	715/513
5,933,829	A *	8/1999	Durst et al.	707/10
5,940,135	A	8/1999	Petrovic et al.	348/493
5,943,423	A	8/1999	Muftic	705/67
5,949,885	A	9/1999	Leighton	380/54
5,953,415	A	9/1999	Nielsen	705/58
6,002,772	A	12/1999	Saito	705/58
6,005,643	A	12/1999	Morimoto et al.	375/240.26
6,006,200	A	12/1999	Boies et al.	705/26
6,018,720	A	1/2000	Fujimoto	705/26
6,035,177	A	3/2000	Moses et al.	725/22
6,175,823	B1 *	1/2001	Van Dusen	705/26
6,434,535	B1 *	8/2002	Kupka et al.	705/24
6,487,663	B1 *	11/2002	Jaisimha et al.	713/193
6,615,247	B1 *	9/2003	Murphy	709/217
6,708,157	B1 *	3/2004	Stefik et al.	705/59
2001/0001854	A1 *	5/2001	Schena et al.	705/27
2001/0032878	A1 *	10/2001	Tsiounis et al.	235/379
2001/0037316	A1 *	11/2001	Shiloh	705/74

(Continued)

FOREIGN PATENT DOCUMENTS

JP 11-66152 A * 3/1999

OTHER PUBLICATIONS

Prosise, J., "How to Keep it a Secret," PC Magazine, vol. 13, No. 13, p. 315, Jul. 1994.*

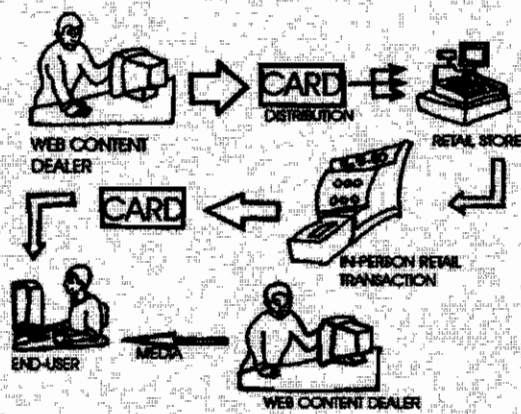
(Continued)

Primary Examiner—Nicholas D. Rosen

(57) **ABSTRACT**

The present invention is an apparatus for the money transactions required in the selling of merchandise or media content on the Internet and uses at least one in-person contact with the buyer. A predefined transaction originating at a real place of business authorizes access to web content or merchandise from a place off the web. Purchasers (end-users) must physically go to a retail location to choose the Internet media or merchandise shopping cart they wish to acquire where age can be verified if necessary and payment can be made with or without a credit card. Content security using a non-audible or invisible code signal sequence(s) can provide traceability as well as absolute anonymity for the purchaser. This apparatus can be used to conduct transactions off the web so that business can be done on the web.

15 Claims, 8 Drawing Sheets



U.S. PATENT DOCUMENTS

2002/0029241	A1*	3/2002	Yokono et al.	709/202
2003/0093335	A1*	5/2003	Silverbrook et al.	705/26
2003/0142035	A1*	7/2003	Immega et al.	713/186
2003/0158790	A1*	8/2003	Kargman	705/26
2003/0200179	A1*	10/2003	Kwan	705/65
2004/0015404	A1*	1/2004	McCarthy	705/26
2005/0192896	A1*	9/2005	Hutchison et al.	705/40

OTHER PUBLICATIONS

Remus, P.C. et al., "Digital Signatures: The Next Step in Electronic Commerce," New hampshire Business Review, vol. 19, No. 10, p. 15, May 1997.*

Gentry, C.R., "Chain Cultivates Farming Niche," Chain Store Age, vol. 76, No. 3, pp. 67-77, Mar. 2000.*

Anon., "Appearing Soon at a Store Near You: An A.T.M. for the Ears," New York Times, vol. CXLIX, No. 51,364, P. D7, Apr. 2, 2000.*

Anon, "Mala Powers: Hollywood Star Still Shines on Walk of Fame," Business Wire, Sep. 27, 1994.*

Dyson, P., "MiiliCent: Digital Equipment's Scrip for Selling Content by the Slice," Seybold Report on Internet Publishing, vol. 2, No. 3, p. 37, Nov. 1997.*

Oser, K., "Wells Fargo Launches ATM Advertising," Direct, vol., 11, No. 5, p. 22, Apr. 1999.*

Buelva, A.J., "Philippines: Union Bank Launches 'Net Banking Initiative," Computerworld (Philippines), Dec. 15, 1999.*

Muhammad, T.K. "Pointing the Way to Cyber-Success," Black Enterprise, Nov. 1996 vol. 27 No. 4 pp 44-46.

Goldstein, A., "Computer City Opens Prototype, in Mesquite, Texas," Dallas Morning News, Nov. 22, 1997, pp 11-12, Regarding Internet.

Microsoft Press Computer Dictionery, 3rd Edition, Microsoft Press, 1997, See p. 82, Definitions. & CD Rom Burner & Recorder.

* cited by examiner

FIG. 1

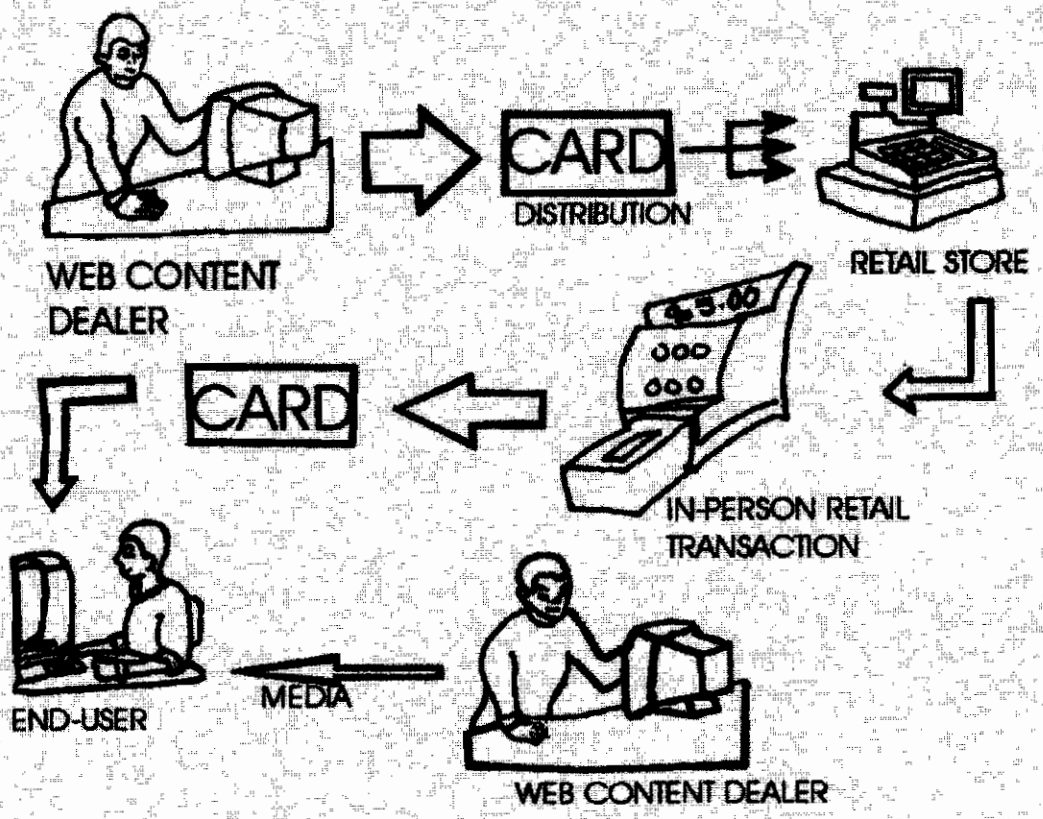

CARD
DISTRIBUTION
WEB CONTENT DEALER
RETAIL STORE
$5.00
CARD
IN-PERSON RETAIL TRANSACTION
END-USER
MEDIA
WEB CONTENT DEALER

FIG. 2

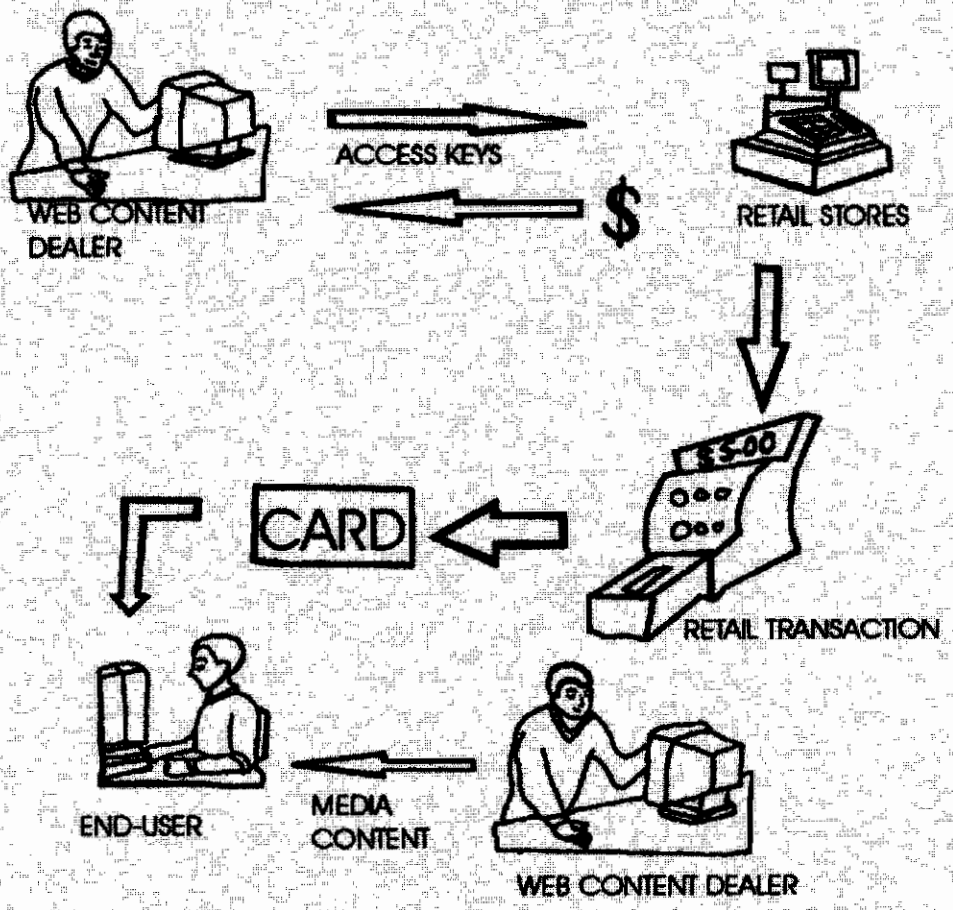

ACCESS KEYS
$
WEB CONTENT DEALER
RETAIL STORES
$-.00
CARD
RETAIL TRANSACTION
END-USER
MEDIA CONTENT
WEB CONTENT DEALER

FIG. 3

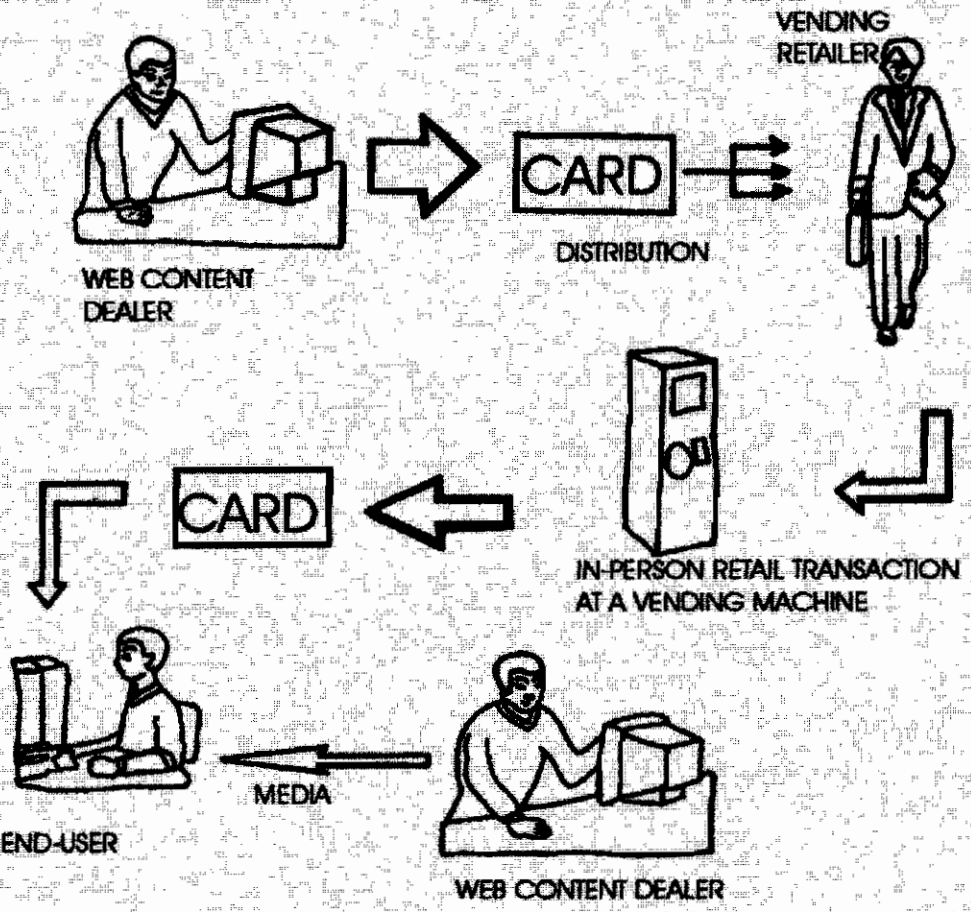

VENDING RETAILER
CARD
DISTRIBUTION
WEB CONTENT DEALER
CARD
IN-PERSON RETAIL TRANSACTION AT A VENDING MACHINE
MEDIA
END-USER
WEB CONTENT DEALER

FIG. 4

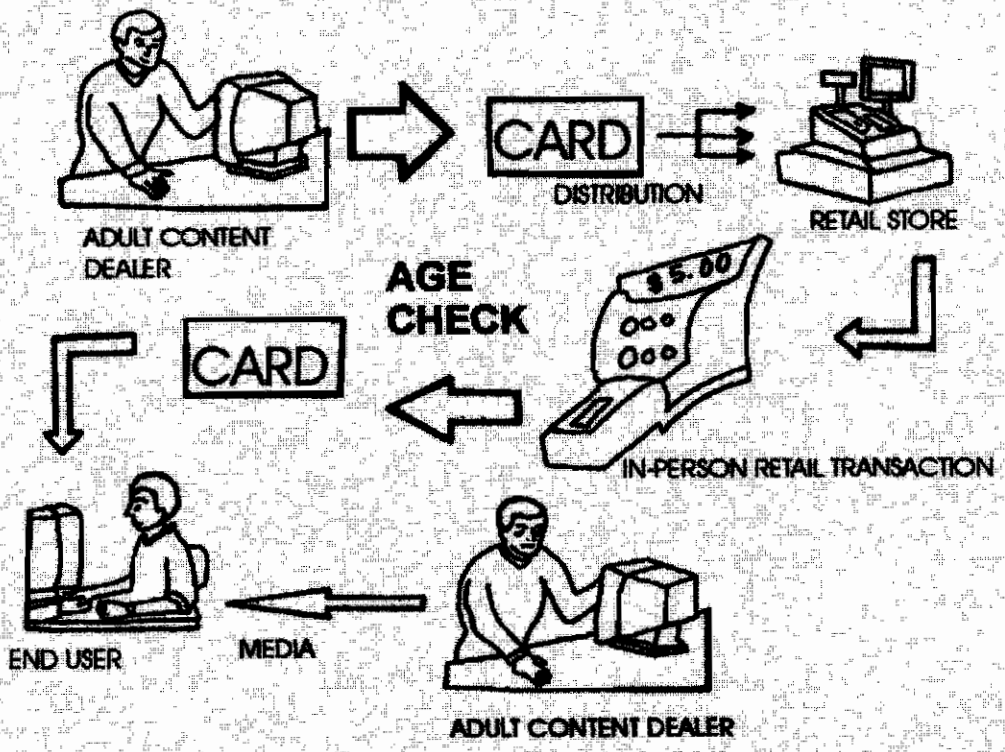

ADULT CONTENT DEALER
CARD
DISTRIBUTION
RETAIL STORE
AGE CHECK
CARD
$5.00
IN-PERSON RETAIL TRANSACTION
END USER
MEDIA
ADULT CONTENT DEALER

FIG. 5

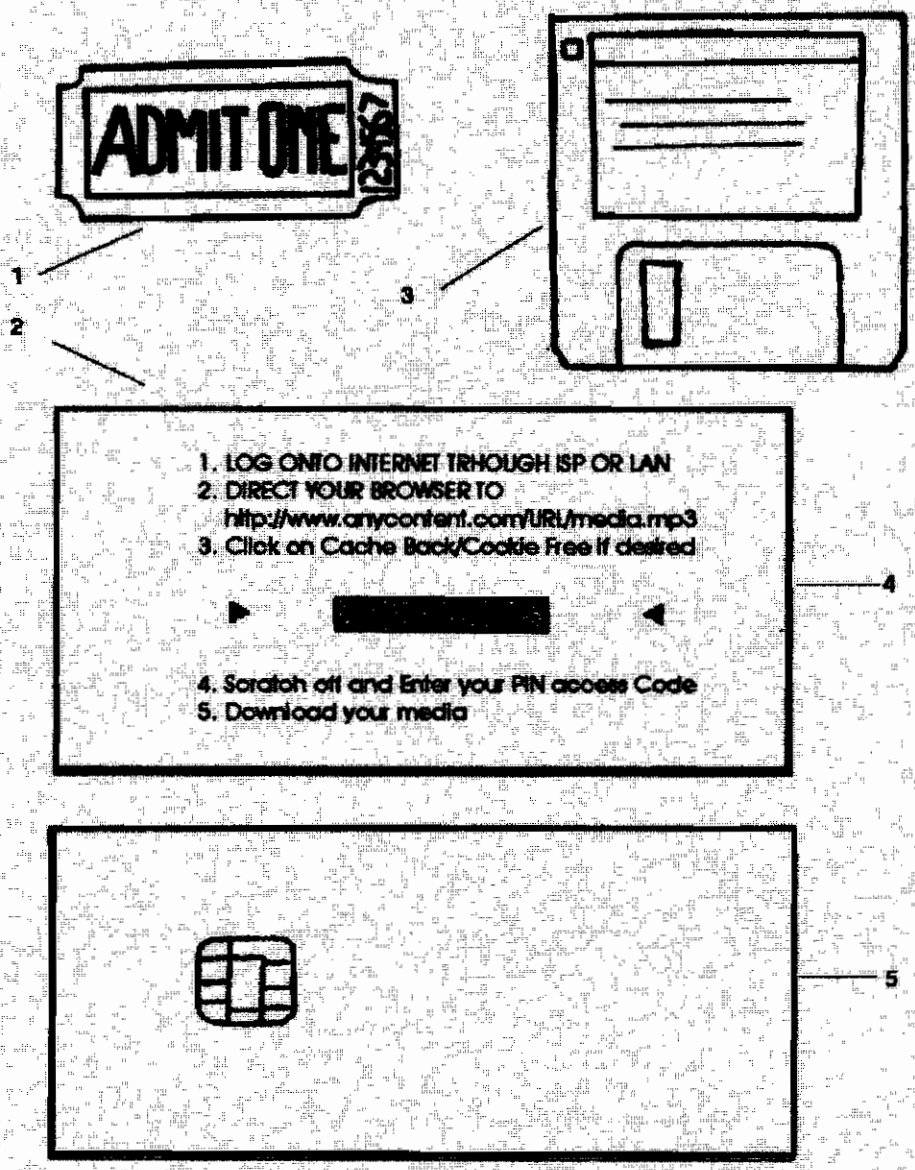

ADMIT ONE
1
2
3
1. LOG ONTO INTERNET THROUGH ISP OR LAN
2. DIRECT YOUR BROWSER TO
http://www.anycontent.com/URL/media.mp3
3. Click on Cache Back/Cookie Free if desired
4
4. Scratch off and Enter your PIN access Code
5. Download your media
5

FIG. 6

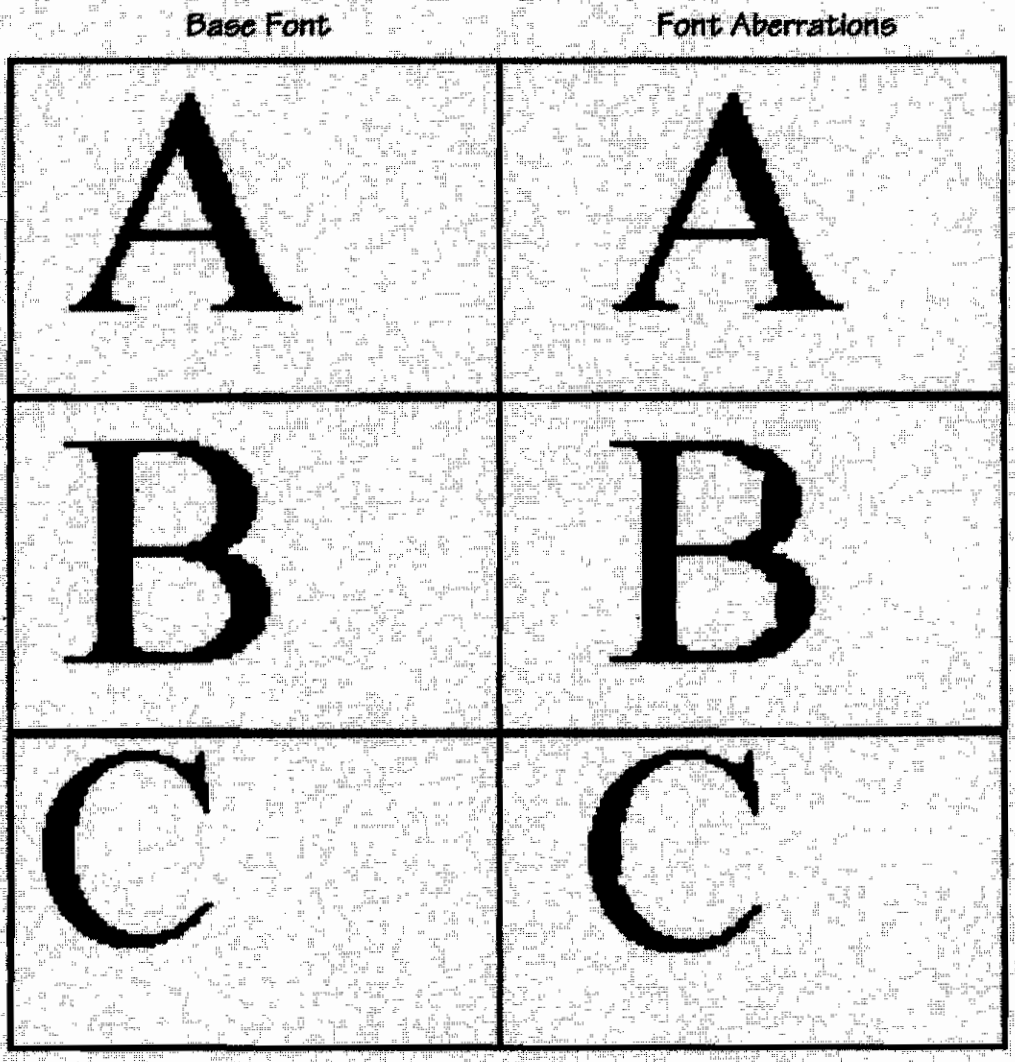


FIG. 7

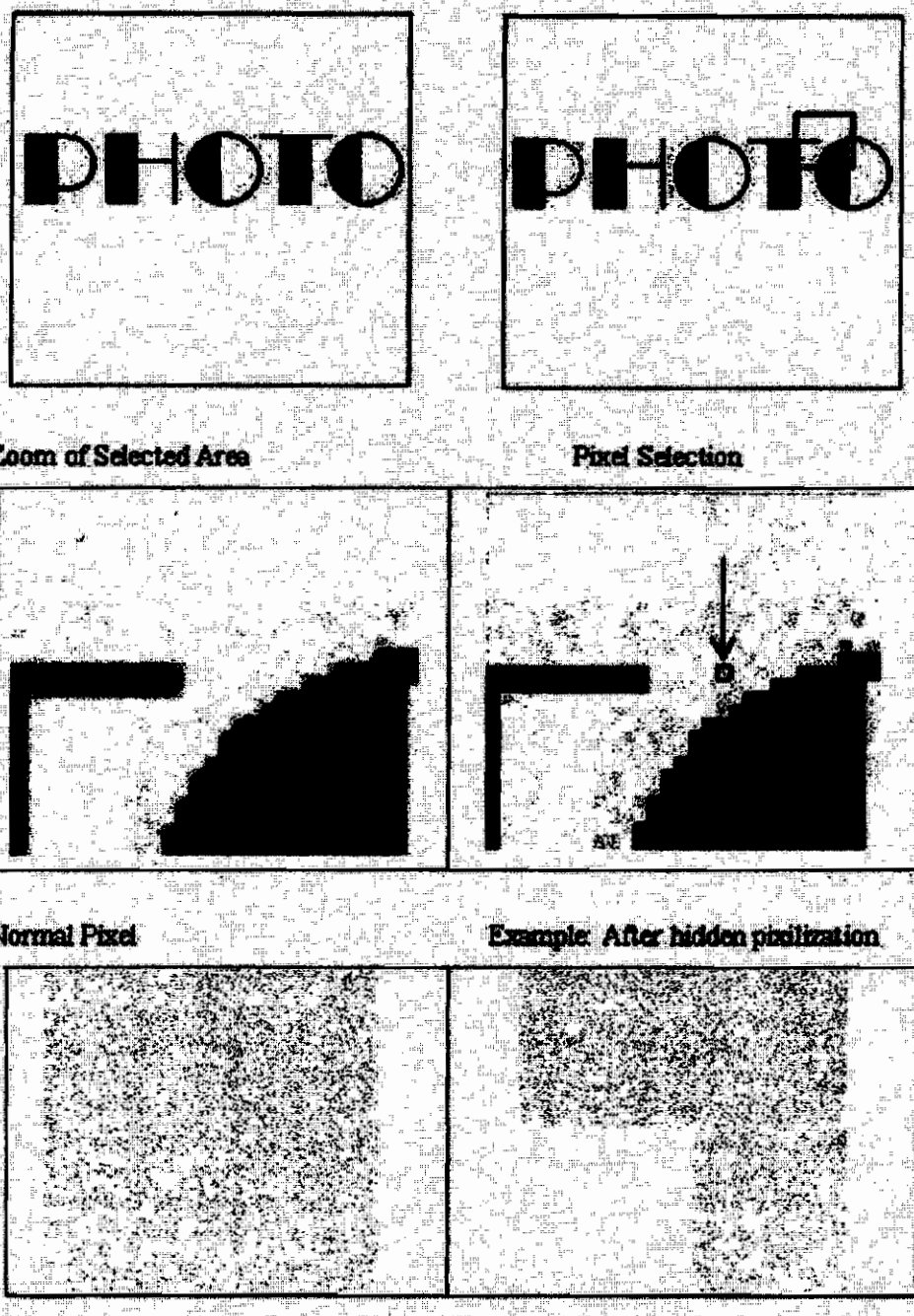
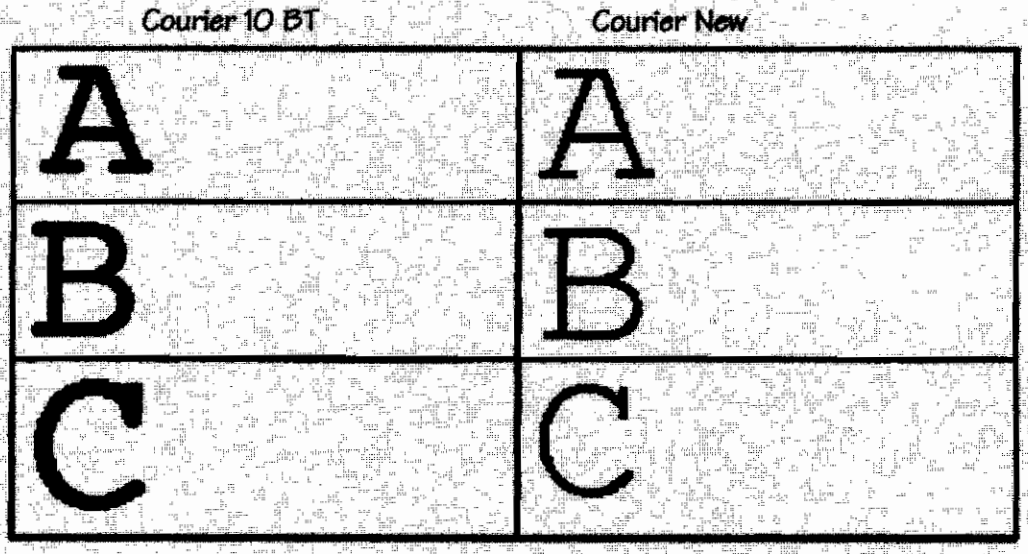


PHOTO
PHOTO
Zoom of Selected Area
Pixel Selection
Normal Pixel
Example: After hidden pixilization

FIG. 8



RETAIL POINT OF SALE (RPOS) APPARATUS FOR INTERNET MERCHANDISING

RELATED APPLICATIONS

Priority is claimed to provisional patent application submitted on Jun. 30, 2000 under same inventor's name, entitled Access Card for Internet Content (ACARD), provisional application No. 60/215,673.

FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not Applicable

SEQUENCE LISTING, TABLE, OR COMPUTER PROGRAM ON CD

Not Applicable

BACKGROUND OF INVENTION

(1) Field of the Invention

This invention relates generally to purchasing systems via a public computer network system (Internet or World-Wide-Web). While the products sold on the Internet are often real and tangible, the market place exists in a virtual realm. To conduct the business of selling in the virtual realm of the Internet, a virtual transaction had to take place; or so it has been thought. This Invention requires non-virtual transactions that take place at a retail point of sale for a means of virtual merchandising.

(2) Related Prior Art

Retail industries can exist anywhere. The historical version of retail was the actual retail point of sale. A retailer established a store where customers could visit, look at merchandise and make purchases. The customer had to visit the store in order to purchase the products. Other forms of retailing have existed like local street vendors, door-to-door salesmen, shop-by-telephone, mail order catalogs, infomercial shop-by telephone, and most recently, the Internet.

To understand the difference between this invention and prior art, one must first be able to understand the differences between retail point of sale and other methods of sale. There is always a time variable involved with merchandising transactions, but one should not make the mistake of assuming that time is the essential element that distinguishes between direct purchases and those on account. The basic formula for establishing a credit account is where the purchase price (P) of a product can be paid at a later time (T), an interest rate (R) can be assessed, and the amount paid $(A)=P(I+R)^T$.

A person may gain extra time to pay for a purchase by using credit, but it is the agreement between parties that one will extend credit to the other that creates a credit account. Time has no meaning in the direct purchase formula (A)=P. For that matter, there is always some lag between the time payment is tendered and possession takes place even if for just split seconds. Sometimes a lag between payment and possession requires a voucher so that the purchaser has some proof that payment has been made. The voucher is usually just a simple sales receipt. Other times it can be a ticket such as for attending a theater or other engagement. The voucher in this case does not represent an account or value of money. The voucher merely represents that the transaction has been completed and the merchandise, whether physical merchandise or simply entertainment, has been authorized.

Retail points of sale transactions involve at least one in-person contact with the buyer. On the Internet, it has always been assumed that this transaction must be conducted virtually on the Internet; after all, the Internet is a virtual realm. With the huge rise in popularity the Internet, there are rising concerns from the public about who should and who should not be able to access certain Internet content such as but not limited to: materials with copyrights such as music, content that is adult in nature, or other restricted access material.

Regulatory authorities and web masters have made attempts to control access through the selling of access rights over the Internet itself. These services are often called subscription based I.D. or age verification services. User names and passwords or other means of secure access have been delivered to consumers after they entered credit card information. This has become an accepted means of control, particularly with Adult Verification systems.

Public Key infrastructure (PKI) is one method that has evolved into a secure and anonymous means of handling web transactions through the uses of encryption, trusted vendors, and trusted banking institutions. PKI methods of Web transactions involve digital signature and money transactions over the Internet. They require a customer, a bank, a merchant, a public archive such as an Internet web site, Certificate Authorization servers, and encryption and decryption of the data.

Most secure web transactions require cookies and Web delivered applets (such as JAVA). A cookie is information that a Web site puts on an end-users hard disk so that it can use the information at a later time.

Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent of all other requests. For this reason, the Web page server has no memory of what pages it has sent to a user previously or anything about previous visits. A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. For example, some browsers store cookies in a file subdirectory and others store cookies as a single text file. Some computers employ programs to ensure that cookies are not used and that the browser caching system will not keep a record of websites visited. A programming sequence flow diagram for a cookie free cache back mini-application may look something like this:

Secure On Routine
Make directory/temp/cachebak
Change directory/cachebak
Copy fat.db cachebak
Folder Copy Temporary Internet Files cachebak
Disable cookies in Internet Options settings
Disable JAVA
Secure Off Routine
Prompt user "download complete"
Compare fat.db to fat.db/cachebak
Compare Temporary Internet Files to Temporary Internet Files cachebak
Delete fat.db
Delete Temporary Internet Files
Copy cachebak fat.db to fat.db
Copy cachebak/Temporary Internet Files to Temporary Internet Files
Enable JAVA
END

Retail Point of Sale Apparatus (RPOS) For Internet Merchandising is a return to the simplistic approach of pre-

Internet ways of doing business, but it is not an obvious approach. As malicious attackers of Internet communications become more common, the Internet security measures become increasingly sophisticated. The RPOS takes away some of the sophistication and uses much simpler yet effective technology in its place. The predefined transaction authorizes access to web content from a place off the web, originates at a real place of business, and is a concept that a trained Internet professional may not be able to grasp immediately; they have been conditioned towards more complicated means of accomplishing the tasks directly on the Internet.

RPOS would not negatively affect any electronic commerce as it currently operates. It would primarily be used in conjunction with current methods. A return to a retail establishment for conducting Web business may hold great promise for Internet security in the future. A search of past practices and inventions reveals a great deal of effort spent on avoiding over-the-counter transactions for Internet e-commerce rather than embracing it as does the RPOS technology.

There are three key questions to be asked when attempting to differentiate the technology:

i. Do they take cash?

ii. Is there an establishment that acts on behalf of the customer for payment that employs non-virtual (Retail point of sale) to complete the transaction?

iii. Does the customer have to physically go to the establishment to buy it?

The field of Internet e-commerce has numerous existing patents. A complete search for prior history was not done prior to this filing but a few similar patents were found through a most basic search of the on-fine USPTO patent databases. They are reference below to help set the stage for one skilled in the art of Internet commerce to understand the differences between RPOS and previous methods.

This invention is not a Prepaid Internet Access Card, such as used to supply the purchaser of minutes on an Internet Service Providers (ISP) system, see examples U.S. Pat. Nos. 5,749,975; 5,987,612; 5,749,075, 5,987,430.

This invention is not merely a method for recording information on a card, computer disk, or other means of recording, see example U.S. Pat. No. 6,076,733. The method of recording might be bar code, magnetic tape, smart card, written inscription, or any means of recording information. This invention is not used to locate a specific URL, but is used to divine the predetermined transaction that provided access to a particular URL location.

This invention is not an organizational Internet access security system whereby business organizations control access to web content of their own employees or to others on a closed network or to generate personalized content pages for specific business purposes, see U.S. Pat. No. 6,076,166.

This invention is not an Internet cash token system used as an anonymous means to get money to spend on the Internet. See examples U.S. Pat. No. 6,076,078; 6,072,870; 6,061,660; 6,042,149.

This invention is not electronic-voucher system, which places a third party URL as the guarantor of funds. See example U.S. Pat. No. 6,058,381.

This invention is not a mobile Internet media content delivery device in which the device itself carries the content. See examples U.S. Pat. Nos. 6,018,720.

This invention is not a means to preview merchandise and set up an account to purchase—as in U.S. Pat. No. 5,918, 213, where the merchandise merely previewed at the point of sale, but then the transaction is conducted as an off the shelf purchase, through typical Internet methods, or phone-in-sale automated means. The retail point of sale apparatus for Internet Merchandising is a new means for conducting the actual transaction that could be added to such a system.

This invention is not a device for delivering media content through on-line programmable smart card authorization such as used in satellite television programming, or Web TV devices, where a home user of the system can call in on the telephone to order Pay-per-view programming. In these systems the smart card both receives and supplies data to the system over a private network. RPOS does not require programming after the initial over-the-counter transaction.

Although the user of the RPOS may be known, it can also be used completely anonymously.

This invention is much like an event ticket to a movie theater or music concert except that the RPOS is specifically used for access (entrance) to Internet merchandising.

While RPOS can facilitate Secure Web Transactions, it is not a method of the transaction, merely an apparatus of divining the existence of a predetermined web transaction. It does not require a trusted vendor, trusted bank, or buyer authentication. While RPOS may facilitate some of the same types of functions mentioned above, it uses a completely new method.

BRIEF DESCRIPTION OF THE INVENTION

This invention is essentially retail point of sale for the Internet. In order to best set the stage for a reader of this patent application to best understand the background of this invention and distinguish it from prior art, several descriptive names of the invention are listed below. This is not intended to be an exhaustive list but merely illustrates some of the ways such an invention can be used. After this list, for the remainder of this document, the Invention will be referred to as the RPOS. Although it involves a voucher system, the voucher need not exist in all circumstances. RPOS can use a disk, paper ticket, memory stick, or any other means of supplying an access key and utility program.

Descriptive Names

1. Internet Content Voucher System
2. Cookie Free Cache Back System Card
3. Prepaid Card for Internet Content Media
4. Web Content Ticket
5. Over-the-counter Internet Sale
6. Simple Anonymity for Internet Content Delivery
7. Face-to-Face Verification System for Divining of Anticipated Internet Transaction
8. Non-Virtual Point of Sale for the Internet
9. Retail Point of Sale Card for Internet Content
10. Internet Authentication Card
11. Internet Adult Verification Card
12. Internet Allocation Card

The RPOS is an "actual point of sale" device for Internet content. Previous waves of invention attempting to satisfy the needs of secure web content on the Internet have delivered many "virtual point of sale" techniques and emphasis has been on the transaction itself and how to exchange money over the Internet.

When considering prior art, the RPOS invention differs most noticeably from previous methods in the way it does not follow the trend to do everything on the Internet and uses "actual point of sale" as the place where a predefined Internet sales transaction takes place. The information provided by web delivered cookies or applets is not required by RPOS because the information is already included; it is hand delivered to the computer by the user.

DESCRIPTION OF INVENTION

A security access key is provided in the form of prepaid card sold as a retail item. The access key has a one time or multiple Internet session use as provided by the seller of the card. Through obtaining the CARD, the purchaser gains access to the website or specific web page(s) intended by the seller for either a defined duration of time or an indefinite duration of time. Any time the end-user (customer) of the CARD is on the Internet, a very simple utility program may be deployed to ensure that there are no changes to the cache content of the customer's computer and no cookies are accepted or transmitted during the delivery of the media content. The utility of the invention is that it provides a method of controlling web access that requires at least one transaction be completed in person. No connection to a banking system for credit referencing is required, no vast system of computer networks is needed to verify anonymity and account status. The actual transaction takes place over-the-counter. The delivery takes place on a computer of the users choice.

The CARD is a voucher system that is used only to authenticate that the user of the card is in fact the one in possession of it. The user of the CARD uses the card to access the content or merchandise from the computer of their choice. As the time required for the user holding the card to receive the desired content is decreased, the need for the CARD itself may become unnecessary. The content itself may be recorded to disk compact disk, cassette, VHS tape, or other recording media: the media may be recorded at the point of sale location.

The content that is recorded may be Internet content media or the content may be the purchase agreement for merchandise. When the content is a purchase agreement for merchandise, the payment can be made for the merchandise by the RPOS. The RPOS assumes responsibility for payment to the Internet vendor and the purchaser specifies the shipping address of such merchandise.

Unlike any previous method of payment for Internet commerce in the past, there is no account, credit, or other means of electronic payment required for the buyer in the transaction. The proof is within the content itself. The content becomes the verification of a sale. Internet merchandisers may provide a verification page for each sale, which they intend to be printed by the user. These types of verification pages are excellent examples of specific URL information that can be determined ahead of time and sold whether it is for merchandise or content media.

When the purchase is for non-prepackaged merchandise such as Content media, the media may be individually licensed with a unique serial number for protection against counterfeiting. Content fingerprinting is one of the methods used. Traditional digital signature may also be used.

Content Fingerprinting

Content fingerprinting could be used for printing secure documents, discouraging unauthorized use, sending secret encoded messages, authentication of modification of documents, counterfeit detection, or other application requiring secure distribution of Internet materials. Content fingerprinting differs from digital signature or digital watermark in that the fingerprinting is not on the file itself but on the content of the file.

In the Industry of Internet publishing, one of the problems has been unauthorized copying, posting or otherwise revealing of sensitive materials for wide distribution. Millions of dollars in uncollected royalties are lost each year. Publishers have no way of detecting the responsible parties who willfully post the materials or otherwise "leak" the materials for wide distribution. The answer to the problem is a mechanism or way to "mark" individual copies of recorded material for licensing so the publishers can feel confident that appropriate royalties are being paid. The "mark" should be something not easily detected or removed.

This document suggests just some basic methods of fingerprinting Internet content: Font Fingerprinting, hidden pixelization, concealed ASCII and non-visible/inaudible codification.

Font Fingerprinting

Bar codes are typically comprised of black and white stripes, yet all that a bar code really represents is a binary code. For Font Fingerprinting of Internet content, hidden binary codes are placed into documents so that a specific record of the content travels with the document. It is much different from digital signature for example where the file itself is tagged and encrypted and can't be read unless the proper keys are used to decrypt the message. For fingerprint marking of the document, the mark stays with the document even after it is properly received and possibly changed.

A base font is modified only slightly so as to not be immediately noticeable to the human eye, yet enough for machine recognition. The base font becomes the "0" of the binary and the modified font is the "1". Any text string can be modified to imprint a binary coded binary (BCB). The decoding is later accomplished using a scanner with a character recognition system capable of distinguishing the font differences.

Font fingerprinting is particularly designed to be most readily used for printed media, but the fingerprinting could also follow a soft copied document provided the file format remains Rich Text Format (.RTF) or better, giving access to the font aberrations. The font set used for printing the "fingerprinted" document must also be available to the computer that receives the document. Future developments could include a highly compressed file format capable of self-decompression that would mask the fact that the Distributed font set is traveling with the document.

Another method of sending a font generated BCB with a softcopy document, not requiring a font subset file, mixes two available fonts that are a close match such as Courier New with 11 point font and Courier 10 BT with a 10 point font. While this combination is readily visible to the naked eye, the text is not noticeably different unless you know what you're looking for. It was just an attempt at finding a good match, but there may be other good system fonts that are a close enough match.

Hidden Pixelization

The format of choice for delivery of images over the Internet has been the jpeg, formally the ISO standard 10918, which keeps the file size for delivery fairly small. All digital images of this type are made up of tiny pixels. For hidden pixelization, a jpeg image is converted to a similar image of a higher resolution (more pixels). In other words any single pixel in the original image is recreated as multiple pixels all of the same color. For example a 320×240=76,800-pixel image becomes a 640×480=307,200 pixel image, or roughly four pixels per one pixel of the original image.

Several of the pixels from these new higher resolution images can then be encoded with a BCB by varying the shades within the 4 pixels only slightly—leaving the neutral color of the original larger pixel essentially unchanged. Any documents delivered over the Internet that contain these images are thereby permanently marked.

This re-pixelization creates four available binary codes in the original pixel. The original color is the "0" code and the slightly changed shade is the "1" of the binary. One of the keys to making this system less detectable is to disguise the encoding by causing the encoded jpeg file to still report to the user that it is still a 320×240 image when in fact it has been changed to a 640×480 image and then report back to the viewing system the proper resolution. If the user resaves the image into a different format such as GIF, the code may or may not be transferred, but as long as images in documents are untouched, the document remains fingerprinted.

Concealed ASCII

ASCII stands for American Standard Code for Information Interchange. ASCII was developed a long time ago and the characters are not always used in the same way on different computer systems. ASCII was originally designed for teletypes and the first 31 characters in today's applications are no longer used as originally intended. Concealed ASCII finger printing takes advantage of the fact that several of them act the same as the ASCII character "032" in many applications. ASCII 32 is the code for a blank space.

ASCII characters 0, 10, and 13 do not display anything on most applications. Character 9 will move to a tab, making a long blank space. 16–25 and 27–31 produce a black area on the screen in some applications and a blank area in others. So do 1–9, 11, 12, 14, and 15 on some applications; however, they often cause error messages in the compiler for many applications.

Concealed ASCII can create a BCB by using the standard ASCII 32 in spaces as the "0" character of the binary and an alternate ASCII 0, 10, or 13 with ASCII 32 as the "1" character of the binary. Example: The quick gray fox jumps over the lazy brown rabbit.

There are nine spaces to use for the BCB in the preceding phrase. The code in the example above could read 010000111. The code for the 2nd, 7th, 8th, and 9th spaces in the phrase could be ASCII 10 followed by ASCII 32. The remaining spaces could simply use ASCII 32. While the concealed ASCII fingerprinting is not printable, it can be used to travel with text of a printable document.

Concealed ASCII can easily be lost when transmitted as plain text over the Internet and other systmes, but many documents are transmitted over the Internet in specific file formats that would maintain specific ASCII sequences not visible to the reader without looking to the particular codes that generated the text.

Non-visible or Inaudible Codification

Analog signals of non-discernable frequencies for human ears or eyes are individually dubbed into audio recordings, which can later identify the origin of the recording. The sights or sounds are created using a frequency, signal generator, or other means of creating analog signals. The analog signals, which cannot be heard by humans on the recording, can be used for distribution of copyright materials such as mp3 music or dubbed into the soundtrack of a video that is distributed on the World-Wide-Web (Internet).

Identical songs or videos by the same artist can become individual versions that are licensed to individuals. Using sensitive digital software and computer sound editing tools available from a number of manufacturers the sights and sounds outside the range of human discernment can later be detected to verify if the recording is in fact licensed and who is the owner of the license. The analog signals essentially encode any individual identification to a song, video, or other media that contains audio or video tracks.

The human sound range is between 20 and 20,000 hertz for a young person and much less for an old person. The human visual range for light lies within a range around 10^9 MHz. Visual analog signals can also be dubbed into digital video recordings. The key to non-visible or Inaudible Codification is merely that that signals are dubbed into the content and not just on the file itself.

Content Fingerprinting Usefulness

Fingerprinting documents is a useful and new idea. The usefulness of the specific methods shown here is greatly diminished when patented and the PTO discloses to the public. The actual methods of fingerprinting really should be kept as "Trade Secrets". The above methods are not fool proof or even sophisticated enough to hold up against even the least sophisticated of hackers. They are merely offered here as examples of how to individually license Internet materials. As industry looks to the Internet for delivery of every kind of copyrighted material, there will be other specific methods of fingerprinting. Fingerprinting Internet delivered media may involve documents, images, videos, sound tracks, or any other type of media that can be produced for the Internet.

Content fingerprinting is not just for watermarking content, it is capable of providing a level of security for transfer of ownership for prepaid media content over a public computer network (Internet). For example, Public Key Infrastructure (PKI) for secure and anonymous means of handling web transactions can be enhanced by variations of hidden content digital signature fingerprinting using visible or audible codes on a first mark on the content that is a first key of a first public/private key pair to indicate that said merchandise is authentic and a second label that is noticeable only by a machine as a second private key of a private/public key pair used to authenticate the delivery of merchandise.

DETAILED DESCRIPTION OF INVENTION

The following drawings provide examples of different applications and construct specifications for the RPOS technology. They are not meant to be inclusive of all uses, they are merely examples.

FIG. 1 uses a flow chart to illustrate a use of the RPOS. The process begins with web content dealers who have content posted to a public computer network (Internet) and have chosen to use RPOS for distribution. The web content dealers may manufacture the card themselves or use a third party. The type of security system used for placing the access key on the card is only important as to the particular level of security that is desired. The web content dealer then distributes the CARD, directly or through distribution channels, to a retail establishment. The retail establishment sells the CARD over the counter to the customer. The dealer, distributor, and retail establishment may use whatever profit margins or price mark-ups as they choose or is agreed upon. The CARD is delivered to the customer like any other retail product. Continuing along the flow chart in FIG. 1 to the customer, the CARD is used to access only the web content that is predefined by the CARD. The purpose of the CARD in this transaction is only to ensure that the user is in possession of it. The transaction takes place through an over-the counter sale.

FIG. 2 uses a flow chart to illustrate an alternate use of the RPOS The process again begins with Web Content Dealers. In this application the Web Content Dealers may or may not subscribe to the RPOS system (i.e. make their own CARDs).

To facilitate the creation of a CARD for the WEB Content Dealers, a retail establishment supplies a computer or terminal as a customer access point, which provides Internet access, and issues a CARD to a customer upon entering the retail establishment. The customer browses the web and looks for content to purchase. Whenever a Web Content Dealer requires some sort of payment and the customer agrees, the customer authorizes payment from the retail establishment and by default the retail establishment agrees to the purchase. The customer is not required to enter his or her own name, credit card payment information, address, or any other information that they do not choose. Upon leaving the establishment, the customer pays the retail establishment the amount required for content received or to be received. The purpose of the CARD in this transaction is only to ensure that the user is in possession of it. The actual transaction takes place through an over-the-counter sale.

The system described in FIG. 2 illustrates a subtle yet important difference from prior art used in Internet commerce, in that Internet access is only required for the customer to choose which media content to purchase and to later retrieve on whatever computer the customer chooses. Internet access is not required during the recording of specific media content locations (URLs); they can be simply written down, picked out from a written menu after having seen the web dealers preview pages, or retrieved as a menu item from the local computer at the check out. Internet access is also not required during the recording of the specific access information, or during the retail transaction. While Internet Access during these processes may be used to facilitate the RPOS processes, it is not required. While the CARD holds some intrinsic value it does not hold any dollar amount information, account information, or other means of payment; the transaction is completed in person at the checkout.

FIG. 3 uses a flow chart to illustrate an alternate use of the RPOS. The process again begins with Web Content Dealers. A Vending Machine Dealer purchases CARDs through normal product distribution channels. Customer purchases the CARD from the vending machine acquiring the ability to access the desired web content. This type of system is not capable of age verification as with over-thecounter sales. Again, the purpose of the CARD in this transaction is only to ensure that the user is in possession of it. The actual transaction takes place through a vending machine.

FIG. 4 illustrates how CARD is used as an age verification system (Adult Check). The process begins with dealers of adult materials on the Internet. A retail establishment (such as video rental store, convenience store, bookstore, adult merchandiser, or other type of store) obtains CARDs through typical distribution channels. Customers purchase the CARD over the counter provided they can prove they are of legal age to do so. Customer physically transports the CARD to a location where customer has access to a computer that is capable of receiving Web content. The customer uses the CARD to obtain access to those specific materials the seller of the CARD intended.

FIG. 5 shows some examples of recording devices that are used or could be modified for use as the media delivery method, access CARD, or to deliver a small cookie-free-cache-back application. Some of these examples have also been patented previously. All that is required for use with the CARD is the ability to deliver Personal Identification Number (PIN) information or other form of security used for access. For optional added anonymity, the CARD may also deliver a small amount of software code to run the mini-Application for Cookie Free Cache Back system. Reference 1 shows an example a of Low-level security access key. Reference 2 shows an example of how a mini-application (applet) can be delivered on floppy prior to accessing content. Reference 3 shows a better security system using a scratch off access key. Reference 4 shows a smart card which could be used to deliver both an access key and mini-application applet. In all of these examples the CARD is not used as money, credit, or cash.

FIG. 6 is an example of Font Fingerprinting where a font subset file must be delivered to the user.

FIG. 7 is an example of Hidden Pixelization for Content Fingerprinting. The hidden pixelization binary fingerprinting or encoded message can be divined using a scanning device capable of detecting the differences.

FIG. 8 illustrates the similarities between the New Courier font and the Courier 10BT font.

What is claimed is:

1. A payment system for itemized Internet merchandise or itemized downloadable media material objects, comprising:

a retail point of sale establishment;

a customer access point at said retail point of sale establishment;

URL information that is an Internet transaction location of said itemized Internet merchandise or itemized downloadable media material objects;

means for accepting payment through an in person transaction with a customer wherein said payment is designated for purchase of said itemized Internet merchandise or itemized downloadable media material objects;

means for storing and retrieving a record on or in a physical medium corresponding to said URL information that is an Internet transaction location of said itemized Internet merchandise or itemized downloadable media material objects;

means for transfer of said physical medium from said retail point of sale establishment to said customer; and

means for Internet transaction authorization on, in, or actuated from said physical medium wherein ownership rights in said itemized Internet merchandise or itemized downloadable media material objects are preselected and transferred to said customer through said transfer of said physical medium.

2. The payment system of claim 1, wherein the retail point of sale establishment further comprises:

a retail store, convenience store, vending machine, parking lot, hallway, lobby, or other physical place to conduct business.

3. The payment system of claim 1, wherein said customer access point at retail point of sale establishment, further comprises:

a checkout, kiosk, cashier's station, cash register, self-check out, self-service, or other means of customer interaction with said retail point of sale establishment.

4. The payment system of claim 1, wherein said means for storing and retrieving a record further comprises:

writing, inscribing, programming, or otherwise placing access information on a card, computer diskette, or other physical means of recordation without requiring access to a public computer network (Internet) during the recording process whether or not access is actually made.

5. The payment system of claim 1, wherein said means for Internet transaction authorization further comprises means to embed a public/private cryptographic key pair corresponding to said Internet transaction authorization on or in said itemized Internet merchandise or itemized downloadable media material objects comprising:

means for embedding a first coded license, serial, or other identifying mark through content fingerprinting on or in said itemized Internet merchandise or itemized downloadable media material objects that uses a code visible, audible, or otherwise noticeable only by machine on a first mark that is a private key of said public/private key pair; and

means for embedding a second coded license, serial, or other identifying mark through content fingerprinting on or in said itemized Internet merchandise or itemized downloadable media material objects that uses a code visible, audible, or otherwise noticeable by human or machine on a second mark that is a public key of said public/private key pair.

6. The payment system of claim **1**, wherein said means for Internet transaction authorization on, in, or actuated from said physical medium wherein ownership rights in said itemized Internet merchandise or itemized downloadable media material objects is transferred, further comprises:

user access terminal on a computer network;

means for retrieval of said itemized Internet merchandise or itemized downloadable media material objects by said user access terminal wherein retrieval is carried out without transmission of or use of cookies on said user access terminal or electronic disclosure, presently or previously, of user information other than IP address of said user access terminal.

7. The payment system of claim **1** wherein said payment further comprises a price wherein said price is at least zero comprising a free sample or any positive amount of payment from said customer to said retail point of sale establishment.

8. Anonymous Internet transaction authorization system or other secure purchase to facilitate the transfer of ownership rights in itemized Internet merchandise or itemized downloadable media material objects, comprising:

itemized Internet merchandise or itemized downloadable media material objects offered by a seller or other distributor on the Internet through an Internet connection;

user access terminal means connected to the Internet, said user access terminal having an IP address; and

means for payment or otherwise completing an Internet sale of said Internet merchandise or media from said seller or other distributor to the user of said user access terminal with no presently or previously required disclosures of user information from said user or said user access terminal other than said IP address.

9. The anonymous Internet transaction authorization system or other security to facilitate the transfer of ownership or rights in Internet merchandise or media of claim **8**, wherein means for payment further comprises:

payment without transmission, reception, or use of cookies on said user access terminal; or without disclosure of user information from or to said seller or distributor other than said IP address; or without disclosure of user information from or to any third party or third party terminal other than said IP address; or without transfer of funds or promise for payment of funds presently from or to said seller or distributor; or without transfer of funds or promise for payment of funds presently from or to any third party or third party terminal.

10. A method of merchandise transfer on a computer network comprising at least one buyer computer on a network for operation by a user desiring to buy at least one product and at least one selling computer on said network operating for a purpose to sell said product, the method comprising the steps of:

creating specific information that is a transaction location of said product, said product comprising networked merchandise or downloadable media material objects represented on said selling computer;

specifying a price wherein said price is specific to said product on said selling computer;

receiving payment of said price through an in person transaction with said user at a retail point of sale location wherein said payment amount is associated to said product;

sending a payment message as a response to said in person transaction either directly or through other computers on said network to said selling computer on said network;

causing an authorization message to be created on said selling computer in or as a result of said payment message that comprises at least said specification of said product and authentication based on cryptographic key(s), said selling computer being programmed to receive said authorization message for verification of said authentication;

causing selling computer, as a result of said selling computer being programmed, to ensure that said authorization message was created using said cryptographic key(s); and

causing transfer of ownership rights in said product to said user desiring to buy said product by granting access or rights to said user on said buyer computer either directly or through other computers on said network, as a result of said authorization message on said selling computer.

11. The method of merchandise transfer on a computer network in claim **10**, wherein said authentication further comprises a method of self authenticating merchandise wherein said method of self authenticating merchandise comprises:

recording a representation of said access message authenticator on or in said product, said representation comprising

a first coded license, serial number, or other identifying mark comprising a public key on or in said product that uses a code visible, audible, or otherwise noticeable by human or machine on a first mark that is a public key of said public/private key pair; and

a second coded license, serial number, or other identifying mark through content fingerprinting on or in said product comprising a private key that uses a code visible, audible, or otherwise noticeable only by machine on a second mark that is a private key of said public/private key pair.

12. The method of merchandise transfer on a computer network in claim **10**, wherein said specific information that is a transaction location of said product further comprises a Uniform Resource Locator (URL).

13. The method of merchandise transfer on a computer network in claim **10**, wherein said specifying a price wherein said price is specific to said product on said selling computer, further comprises a price set to at least zero, comprising a price of free or any positive amount.

14. The method of merchandise transfer on a computer network in claim **10**, wherein said in person transaction at a retail point of sale location further comprises selling a prepaid card wherein said prepaid card is also specific to said product.

15. The method of merchandise transfer on a computer network in claim **10**, wherein said retail point of sale location further comprises a retail store, convenience store, vending machine, parking lot, hallway, lobby, or other physical place to conduct business.

* * * * *